GENERAL DYNAMICS

Trusted Provider of Cyber Solutions

7th Annual GFIRST National Conference

The Eye of the Beholder--Cyber Situational Awareness

Vince Holtmann

August 11th

GENERAL DYNAMICS
Strength On Your Side™

Session Map

1. Why situational awareness?
2. Ideas and approaches
   a) Normalize, Develop, Create, Reduce, and Provide
3. Technology demonstration

Technology Overview

Why Situational Awareness?

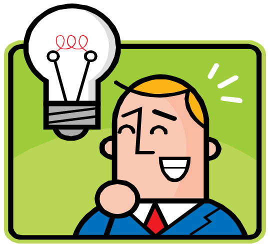
Current Shortfalls

- Lack of Common Operational Picture (COP)
- Inability to visualize multiple dissimilar data sets in one common framework
- Inability to merge operations, logistics, and C2 pictures
- Inability to provide focused visual analytics

Proposed Benefits of Situational Awareness

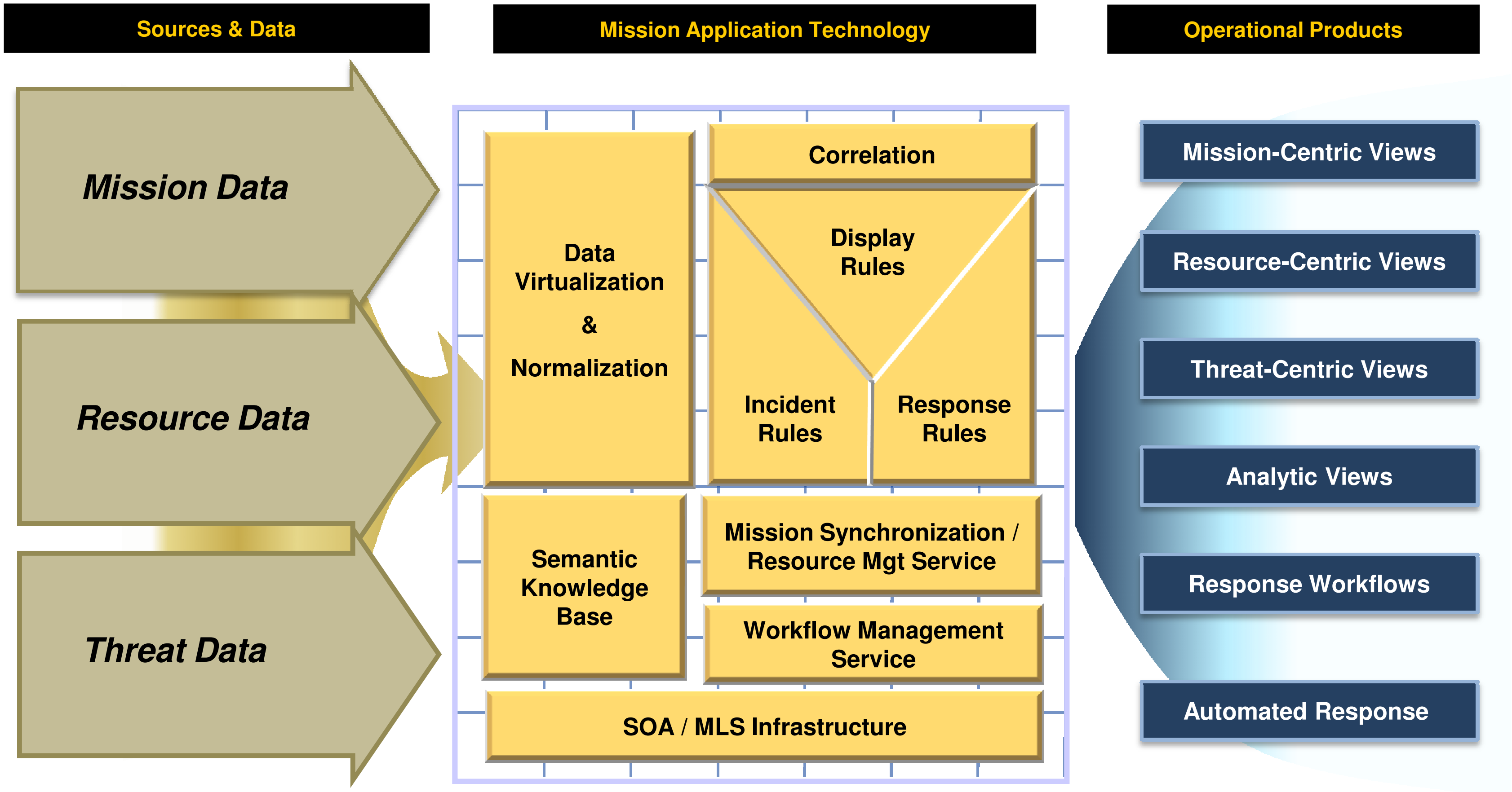
- Supports decision or Course of Action (COA) selection
- Encourages collaboration and data sharing
- Provides a critical component to achieving cyber Information Dominance
- Enables automation of manual tasks
- Leverages dissimilar data sets/reporting tools into one visualization framework

Ideas and Approaches



1. **Normalize** and overlay threat, mission, and resource data to provide a rich situational awareness picture.
2. **Develop** trust relationships between data sharing organizations to increase data fidelity and a wider aperture for domain situational awareness.
3. **Create** a collaboration framework to decrease the duplication of knowledge creation.
4. **Reduce** anomalies and focus resources on high priority tasks.
5. **Provide** the right perspectives for the intended audience, the data is there how would you like to visualize.

Objective Architecture



Sources & Data

Mission Application Technology

Operational Products

Mission Data

Resource Data

Threat Data

Data Virtualization & Normalization

Correlation

Display Rules

Incident Rules

Response Rules

Semantic Knowledge Base

Mission Synchronization / Resource Mgt Service

Workflow Management Service

SOA / MLS Infrastructure

Mission-Centric Views

Resource-Centric Views

Threat-Centric Views

Analytic Views

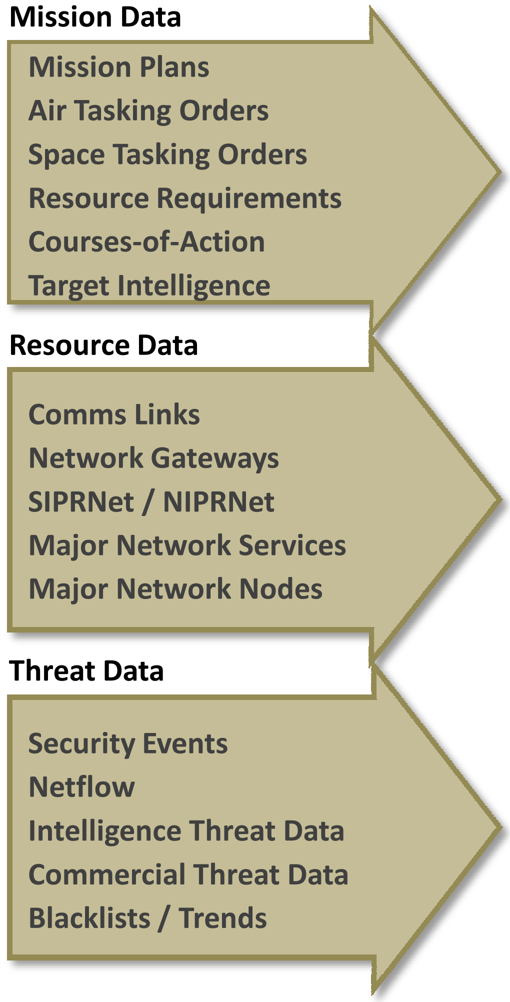
Response Workflows

Automated Response

Awareness ✦ Analysis ✦ Action

Data Normalization and Correlation

1. **Normalize** and overlay threat, mission, and resource data to provide a rich situational awareness picture-Mission Assurance
   - ○ Data Virtualization provides abstraction of federated data stored in multiple data bases
     - ▪ Exposes data via web services
     - ▪ Resolves any data conversions to a Common Data Model at query time
     - ▪ Removes Extract, Transform, and Load (ETL) prior to queries
     - ▪ Enables single query to offload processing on multiple databases
       - ❑ Single aggregated query result returned
       - ❑ Results are only returned not raw event data (unless required)


Mission Data

Mission Plans
Air Tasking Orders
Space Tasking Orders
Resource Requirements
Courses-of-Action
Target Intelligence

Resource Data

Comms Links
Network Gateways
SIPRNet / NIPRNet
Major Network Services
Major Network Nodes

Threat Data

Security Events
Netflow
Intelligence Threat Data
Commercial Threat Data
Blacklists / Trends

Sources & Data

Normalized Data Types

1. **Mission Data--** may include mission plans, tasking orders, fragmented orders, intelligence data, COAs, or resource requirements. This data is used to develop Mission-Centric views (Mission Assurance) showing how existing or planned missions may be affected by ongoing Cyber threats, events, or resource status changes.

2. **Resource Data--** critical infrastructure components, which may include communications links, network services, critical nodes, or gateways. This data is used to develop Resource-Centric views showing how ongoing Cyber threats or events and more may affect existing resources importantly how these map to missions and business objectives.

3. **Threat Data --**this data source contains three primary categories to provide threat situational awareness.
   - Security Event Data – includes security event data generated by commercial SIEMs, such as Arcsight, Symantec, McAfee, or sensors (firewalls, IDS, IPS, routers, security appliances, etc.) distributed throughout the enterprise.
   - Netflow Data – includes source and destination IP addresses, ports, protocol, and packet data from network sensors collecting Netflow data. Netflow data is queried based on defined rule sets and analytic requirements. Summary flow data can be displayed to help identify top talkers or other network anomalies. Flow data related to specific events or IP addresses can be generated and displayed to support detailed analysis.
   - Threat/Vulnerability Data – may include current threat and vulnerability data from external (or internal) sources such as Symantec Deepsight, Cymru, Cyber-TA, National Vulnerability Database (NVD), Top Ten threat lists, Watch Lists, Emerging Trends, etc. It may also include non-Cyber threat data including State Department, Intelligence, or other threat sources that can be correlated with specific security event data or used to assist operators in predictive analysis.

Data Sharing

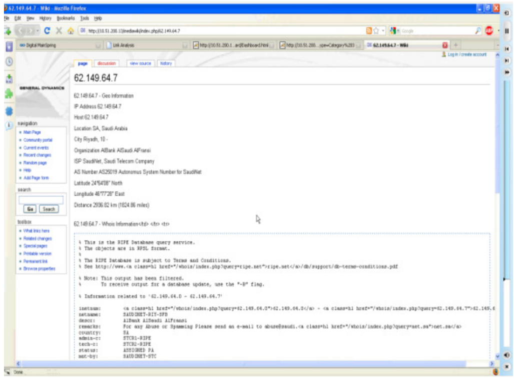
1. **Develop** trust relationships between data sharing organizations to increase data fidelity and a wider aperture for domain situational awareness.
   - ○ Current example: Defense Industrial Base Collaborative Information Sharing Environment (DCISE)
     - ▪ Entrance criteria to ensure only “authorized” parties are granted access
     - ▪ Contractual/Non-disclosure agreements
     - ▪ Control the data via multi-level security, segmented data, and rights restricted
     - ▪ Process for data correlation
     - ▪ Standard for data dissemination and validation

Data Sharing

1. Key Components
   - Ease of access
     - Web-based portal
     - Identification of data producers and consumers (pedigree validation)
   - Maintaining fidelity, confidentiality, and chain of custody
     - Fidelity control
       - What are the criteria for improving data fidelity
       - What are the validation techniques
     - Confidentiality control
       - Multi-level security, data segregation, auditing, access control, etc.
     - Chain of Custody
       - Investigative data must be left in tack to support litigation
         - Disk duplication, virtual machine creation, data mirror, etc.

Knowledge Management

1. **Create** a collaboration framework to decrease the duplication of knowledge creation.
   - Wiki and blogs provide utility for textual knowledge creation and sharing
     - Constant refinement can be structured or unstructured (verification and validation)
     - Semantic metadata tagging provides context between data entities
     - Self-forming ontologies can align directly with business model and objectives
     - Rapidly developed with "care and feeding" at necessity of users



62.149.64.7

62.149.64.7 - Geo Information

IP Address 62.149.64.7

Host 62.149.64.7

Location SA, Saudi Arabia

City Riyadh, 10 -

Organization AlBank AlSaudi AlFransi

ISP SaudiNet, Saudi Telecom Company

AS Number AS25019 Autonomus System Number for SaudiNet

Latitude 24°64'08" North

Longitude 46°77'28" East

Distance 2936.82 km (1824.86 miles)

62.149.64.7 - Whois Information</td> </tr> <tr>

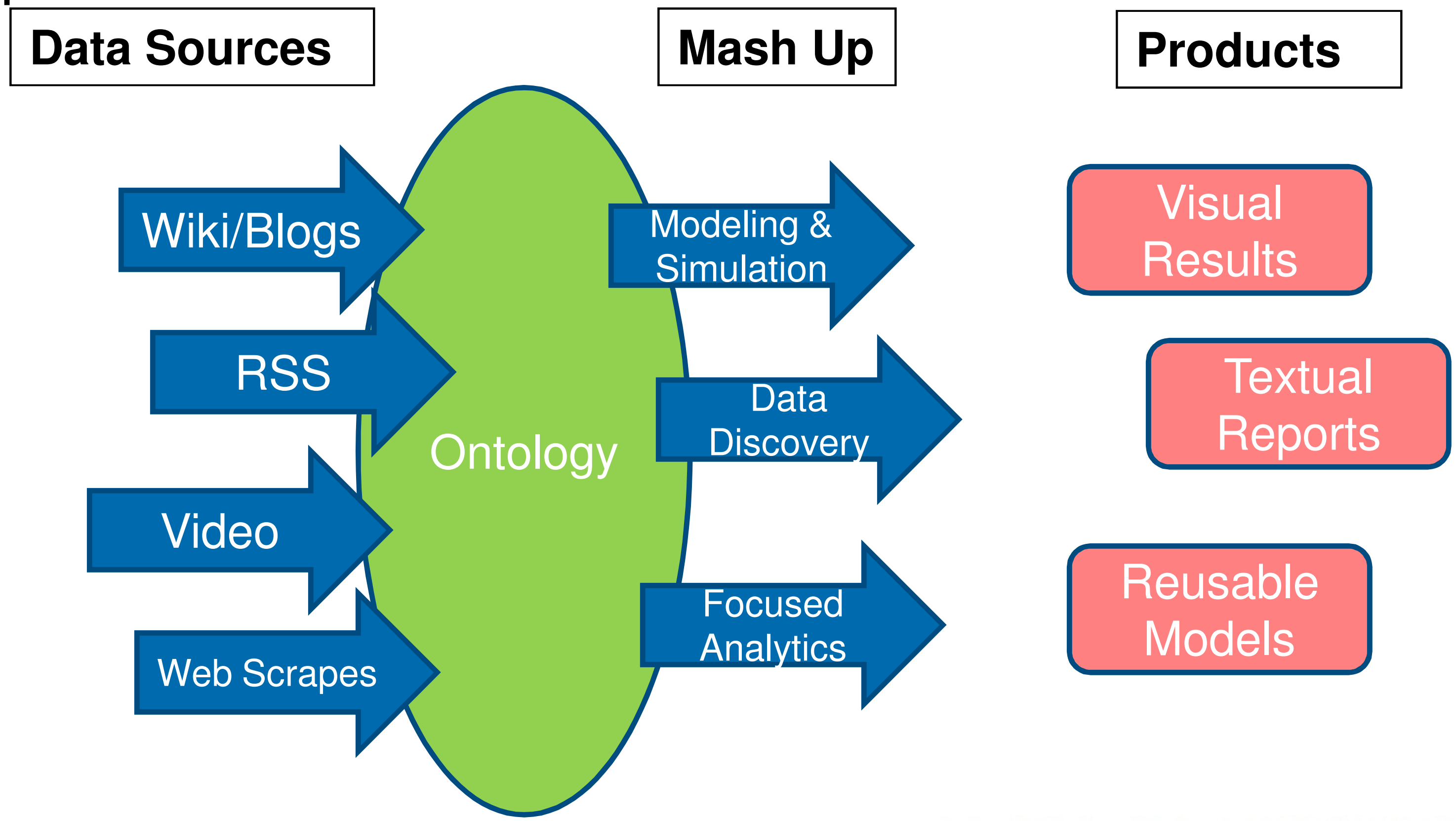
```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.<a class=hl href="/whois/index.php?query=ripe.net">ripe.net</a>/db/support/db-terms-conditions.pdf

% Note: This output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '62.149.64.0 - 62.149.64.7'

inetnum:        <a class=hl href="/whois/index.php?query=62.149.64.0">62.149.64.0</a> - <a class=hl href="/whois/index.php?query=62.149.64.7">62.149.6
netname:        SAUDINET-RIY-SFB
descr:          AlBank AlSaudi AlFransi
remarks:        For any Abuse or Spamming Please send an e-mail to abuse@saudi.<a class=hl href="/whois/index.php?query=net.sa">net.sa</a>
country:        SA
admin-c:        STCR1-RIPE
tech-c:         STCR2-RIPE
status:         ASSIGNED PA
mnt-by:         SAUDINET-STC
```

http://www.youtube.com/watch?v=H8BmiWcaxyg&feature=related (metadata vid)

Knowledge Management

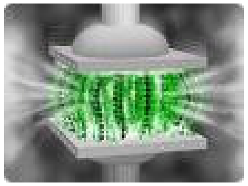
1. Using knowledge base as a start

- Moving from ontology to more advanced information exploration and data awareness



GENERAL DYNAMICS
Strength On Your Side™

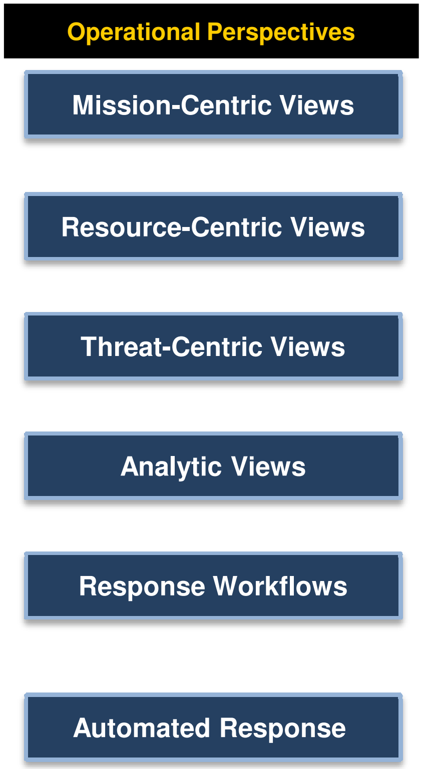
Reduce



1. **Reduce** anomalies and focus resources on high priority tasks.
   - Develop the data hierarchy
     - Leverage multiple similar sources, correlate, and increase data validity through a common data model
       - Leverage previously filtered and aggregated sources to reach “top of the pyramid” for most representative view
         - Retreat to granular data sources for more detailed investigation of data pedigree, filter settings, and collection points when necessary
       - Reduce false positives through alert correlation and rule based methodologies

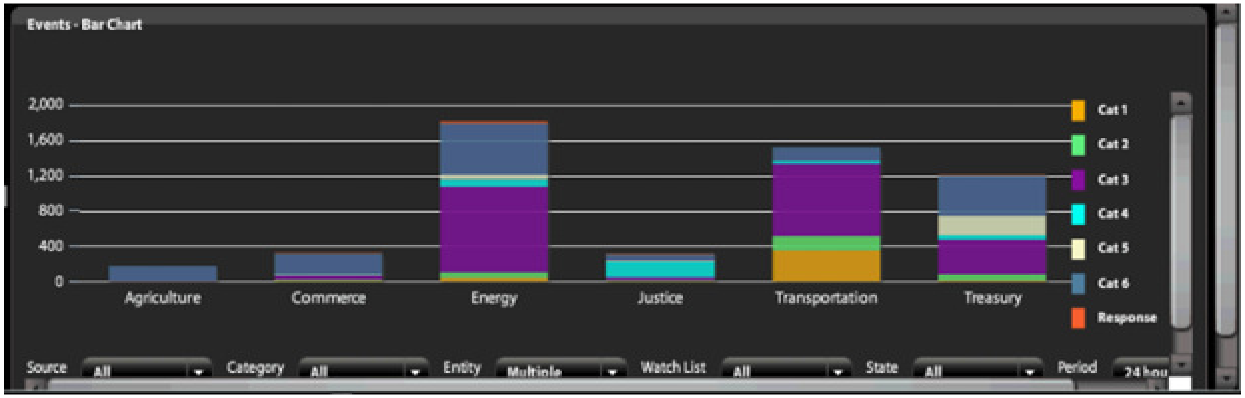
Data Perspectives

1. **Provide** the right perspectives for the intended audience, the data is there how would you like to visualize.
   - User Defined Operational Picture
   - Common Operational Picture
   - User Perspective
   - Etc…..
     - Provide “Static” view for quick look data
       - Commanders/Floor Chief operations view
     - Move to user definable perspective focused on most usable presentation for results
     - Create perspectives per job function…align data as necessary to present result



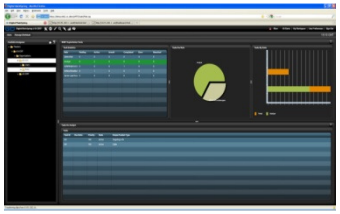
Mission Views

1. **Mission-Centric Views--mission focused views oriented within a dashboard illustrate the effects of ongoing Cyber activity on planned and ongoing missions. The goal is to be able to identify significant activity that may affect current or planned operations and identify appropriate COAs and responses to mitigate the effects.**
   - Sources of Data
     - DHS event handling categories per organization
     - DoD task orders (ITO, ATO, AOD, STO, CTO, FragO), ISR inputs, INTEL, DMPC/BE Numbers, MISREP, and SITREP
   - Data Usage
     - Present major mission/organization locations, objectives, and availability



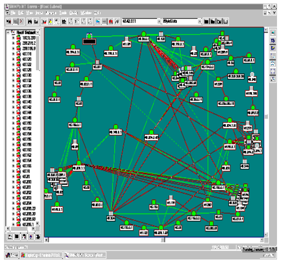
Source All | Category All | Entity Multiple | Watch List All | State All | Period 24 hou

Resource Views

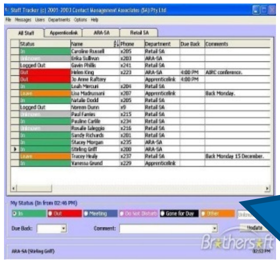


1. **Resource-Centric Views—these views represent critical resources that are identified by the customer and tracked in real-time to show status/ability to support missions and business objectives. Link, node status, sensor feeds, and human capital workload are tracked and reported as critical elements that enable mission success.**
   - Sources of Data
     - NetCool, HP OpenView, CiscoWorks, IMS, SysLog, SNMPc, etc.
   - Data Usage
     - Align critical resources with mission/business objectives
     - Provide automated alerts based on availability status such as over allocation
     - Leverage existing monitoring tools to provide complete resource picture

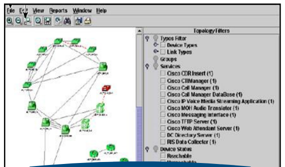
Computing



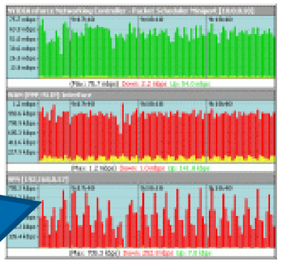
People



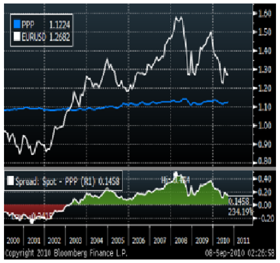
Routing



Bandwidth

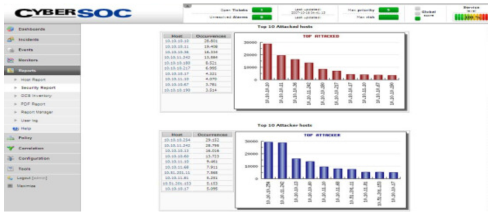


Dollars



Data Sources

Threat-Centric Views



Top 10 Attacked hosts

Host	Occurrences
10.10.10.10	26.801
10.10.10.11	19.408
10.10.10.38	16.334
10.10.11.242	13.884
10.10.10.180	8.521
10.10.10.217	6.995
10.10.10.17	4.321
10.10.11.10	4.070
10.10.10.67	3.781
10.10.10.190	3.514

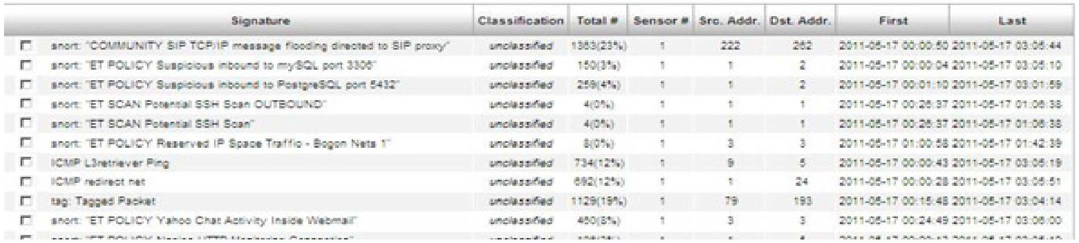
Top 10 Attacker hosts

Host	Occurrences
10.10.10.254	29.152
10.10.11.242	28.798
10.10.10.13	16.016
10.10.10.60	13.723
10.10.11.10	9.461
10.10.11.68	7.911
10.81.201.11	7.868
10.10.11.81	5.281
10.51.201.153	5.153
10.10.10.17	5.095

1. **Threat-Centric Views—these views represent the combination of security, anomaly, black list, and many other data sources that provide perspectives on the contested environment.**
   - Sources of Data
     - ArcSight, Symantec AV/Endpoint Protection, McAfee HBSS, Netflow, Snort/Ossim, TruDetect, IntruShield, Real Secure, Sidewinder, Pix, etc.
     - Symantec Deepsight, Cymru, Cyber-TA, National Vulnerability Database (NVD), Top Ten threat lists, Watch Lists, Emerging Trends, etc.
   - Data Usage
     - Pull incident information from detailed forensic analysis and discovery
     - Automatically report on malicious activity, announcement of zero day
     - Share threat vector, associated patches
     - Integrate local and distributed SIEM sensors
     - Push and pull to unified/shared threat database
     - Align predictive analytics and adaptive rules to become more proactive

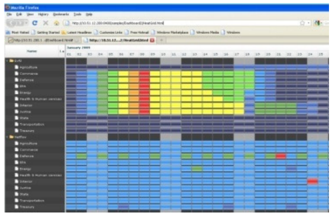
McAfee
Proven Security™

symantec.



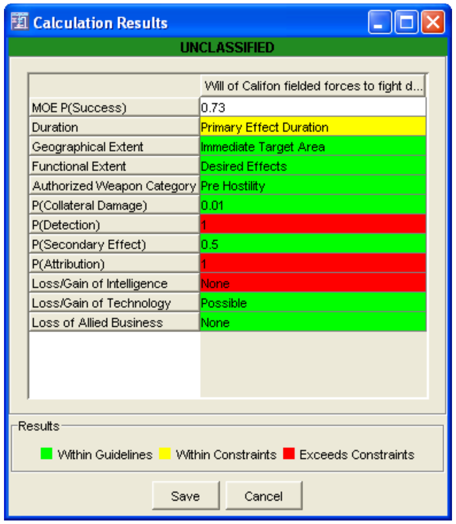
	Signature	Classification	Total #	Sensor #	Src. Addr.	Dst. Addr.	First	Last
□	snort: "COMMUNITY SIP TCP/IP message flooding directed to SIP proxy"	unclassified	1383(23%)	1	222	262	2011-05-17 00:00:50	2011-05-17 03:06:44
□	snort: "ET POLICY Suspicious inbound to mySQL port 3306"	unclassified	150(3%)	1	1	2	2011-05-17 00:00:04	2011-05-17 03:06:10
□	snort: "ET POLICY Suspicious inbound to PostgreSQL port 5432"	unclassified	259(4%)	1	1	2	2011-05-17 00:01:10	2011-05-17 03:01:59
□	snort: "ET SCAN Potential SSH Scan OUTBOUND"	unclassified	4(0%)	1	1	1	2011-05-17 00:26:37	2011-05-17 01:06:38
□	snort: "ET SCAN Potential SSH Scan"	unclassified	4(0%)	1	1	1	2011-05-17 00:26:37	2011-05-17 01:06:38
□	snort: "ET POLICY Reserved IP Space Traffic - Bogon Nets 1"	unclassified	8(0%)	1	3	3	2011-05-17 01:00:58	2011-05-17 01:42:39
□	ICMP L3retriever Ping	unclassified	734(12%)	1	9	5	2011-05-17 00:00:43	2011-05-17 03:06:19
□	ICMP redirect net	unclassified	692(12%)	1	1	24	2011-05-17 00:00:28	2011-05-17 03:06:51
□	tag: Tagged Packet	unclassified	1129(19%)	1	79	193	2011-05-17 00:15:48	2011-05-17 03:04:14
□	snort: "ET POLICY Yahoo Chat Activity Inside Webmail"	unclassified	450(8%)	1	3	3	2011-05-17 00:24:49	2011-05-17 03:06:00

Analytic Views



1. **Analytic Views--additional visualization displays link to more detailed source/intelligence data and provide further analytic capability. Trending views are placed within this category to present propagation of threats, periodicity metrics, bar charts, pie charts, correlated elements, etc. Analysts can drill down from selected cells to network analysis data, showing relationships of event source and destination IP addresses, or to detailed Event Data, which links to a knowledge base to show analyst notes and pertinent data related to the event.**

    - Sources of Data
        - All mission, threat, and resource sensor feeds that provide value
        - Modeling and simulation tools can be added for scenario exploration
        - Custom algorithms, db queries, and predictive analytics will fit here as well



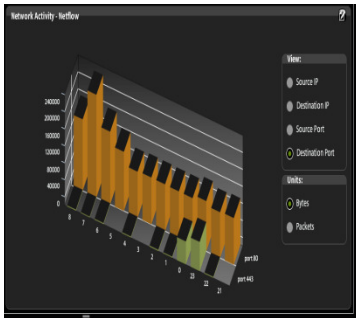
Calculation Results

UNCLASSIFIED

	Will of Califon fielded forces to fight d...
MOE P(Success)	0.73
Duration	🟨 Primary Effect Duration
Geographical Extent	🟩 Immediate Target Area
Functional Extent	🟩 Desired Effects
Authorized Weapon Category	🟩 Pre Hostility
P(Collateral Damage)	🟩 0.01
P(Detection)	🟥 1
P(Secondary Effect)	🟩 0.5
P(Attribution)	🟥 1
Loss/Gain of Intelligence	🟥 None
Loss/Gain of Technology	🟩 Possible
Loss of Allied Business	🟩 None

Results

🟩 Within Guidelines 🟨 Within Constraints 🟥 Exceeds Constraints



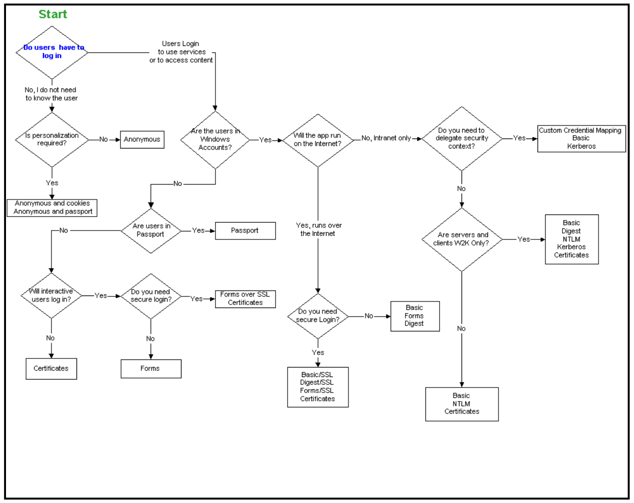
Network Activity - Netflow

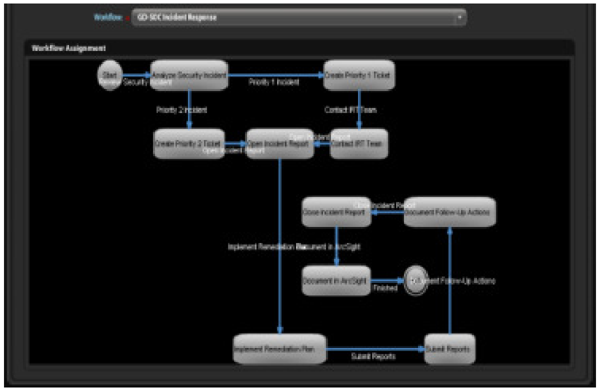
View:
○ Source IP
○ Destination IP
○ Source Port
● Destination Port

Units:
● Bytes
○ Packets

Workflow Views

1. **Workflow Views—provides localized process, tactics, techniques, and procedures at the fingertips of users.**
   - Added benefits
     - Elevates the efficiency and skill level of the entire team
     - Ensures any customer requirements for data/event/task handling (e.g. chain of custody) are followed
     - Allows management to track status of process flow and reprioritize in mid stream if a higher priority surfaces
     - Workflow engine must be user configurable for “on the fly” changes to process


Start
Do users have to log in
Users Login to use services or to access content
No, I do not need to know the user
Is personalization required?
No
Anonymous
Yes
Anonymous and cookies
Anonymous and passport
Are the users in Windows Accounts?
Yes
No
Will the app run on the Internet?
No, Intranet only
Do you need to delegate security context?
Yes
Custom Credential Mapping
Basic
Kerberos
No
Are users in Passport
Yes
Passport
No
Yes, runs over the Internet
Are servers and clients W2K Only?
Yes
Basic
Digest
NTLM
Kerberos
Certificates
Will interactive users log in?
Yes
Do you need secure login?
Yes
Forms over SSL
Certificates
No
No
Certificates
Forms
Do you need secure Login?
No
Basic
Forms
Digest
Yes
Basic/SSL
Digest/SSL
Forms/SSL
Certificates
No
Basic
NTLM
Certificates



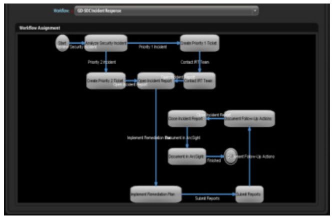
Workflow: GD-SOC Incident Response

Digital MainSpring

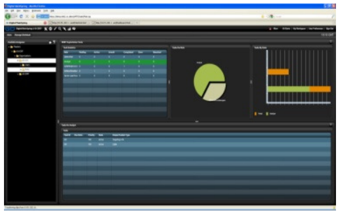
Cyber Situational Awareness, Mission Planning and Execution

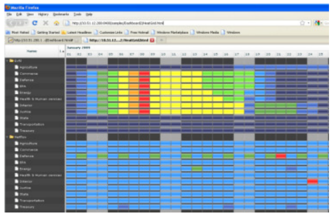
Overview:

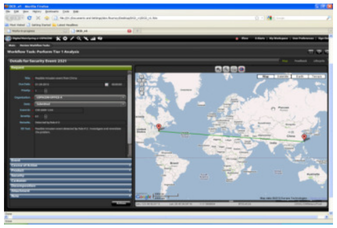
Manages incident response and supports decision making, course of action development and tasks the analyst workload to efficiently use available resources. It integrates with legacy systems and data sources.



DISA
Defense Information Systems Agency
DoD Network Information Center



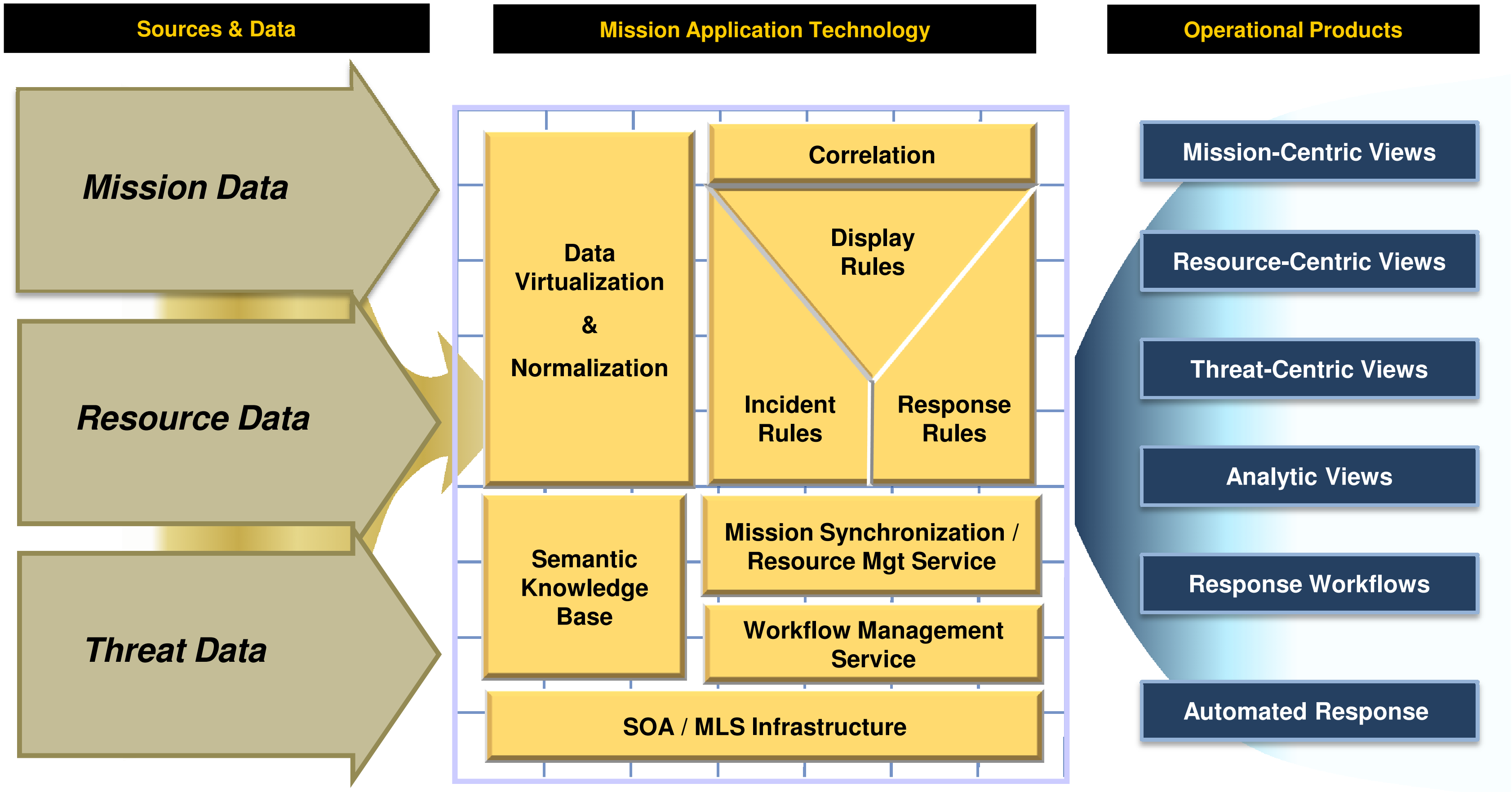




Solutions:

- Open Service Oriented Architecture enabling:
  - Field configurable workflows and rules
  - Rapid ingest and federation of diverse data sources to provide data as a service
  - Incident response, display and metadata tagging rules
  - Analysis agents and tools
  - Visualization displays
  - Automated response for dynamic defense

Objective Architecture



Awareness ✦ Analysis ✦ Action

GENERAL DYNAMICS
Strength On Your Side™

Questions Comments

Thanks for attending!

Contact Information

Vince Holtmann

Vincent.Holtmann@gd-ais.com

210-932-5522

General Dynamics

Advanced Information Systems